IN THE CLAIMS

Please amend claims 19, 24, 41, 46, 65 and 70 as indicated below.

The listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

Claim 1 (previously presented) A method for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name comprising the steps of:

configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name;

configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name;

establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy; and

associating said tunnel with a group in said group database based on said member name such that only one copy of said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server node tunnels associated with said group.

Claim 2 (original) The method as recited in claim 1 further comprising the step of:

configuring a tunnel definition database in said server node, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name.

Claims 3-4 (canceled)

Claim 5 (original) The method as recited in claim 1, wherein said list of members associated with said group name comprise an ID type and an ID of each member associated with said group name.

Claim 6 (original) The method as recited in claim 5, wherein said ID type is an Internet Key Exchange (IKE) defined ID type, wherein said list of members is a non-contiguous list of IKE defined ID types.

Claim 7 (original) The method as recited in claim 5, wherein said ID is a login ID.

Claim 8 (original) The method as recited in claim 5, wherein said ID is a specified name.

Claim 9 (previously presented) The method as recited in claim 2, wherein configuring said tunnel definition database in said server node comprises establishing said server node and said client node as the two end points of said tunnel.

Claim 10 (original) The method as recited in claim 9, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a GUI.

Claim 11 (original) The method as recited in claim 9, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a command line interface.

Claim 12 (original) The method as recited in claim 1, wherein said group database in said server node comprises said group name and an ID type of each member of said group name and an ID of each member of said group name.

Claim 13 (original) The method as recited in claim 12, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a GUI.

Claim 14 (original) The method as recited in claim 12, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a command line interface.

Claim 15 (original) The method as recited in claim 12, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through configuration files.

Claim 16 (original) The method as recited in claim 1, wherein said rules database in said server node comprises said group name, a group name ID type and a security policy pointer.

Claim 17 (original) The method as recited in claim 16, wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a GUI.

Claim 18 (original) The method as recited in claim 16, wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a command line interface.

Claim 19 (currently amended) ~~The method as recited in claim 1 further comprising the step of:~~ A method for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name comprising the steps of:

configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name;

configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node

has a single security policy for each of the plurality of tunnels associated with said group name;

establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy;

associating said tunnel with a group in said group database based on said member name such that only one copy of said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server node tunnels associated with said group; and

activating said tunnel, wherein activating said tunnel comprises the steps of:

sending a security policy stored in a policy database of said client node by said client node to said server node;

sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node;

sending a first nonce by said client node to said server node;

sending a second nonce by said server node to said client node;

sending a first ID by said client node to said server node; and

sending a second ID by said server node to said client node.

Claim 20 (original) The method as recited in claim 19, wherein said first and second nonce are used to generate key material for said server and client node, respectively.

Claim 21 (original) The method as recited in claim 19, wherein said policy database in said client and server node are configured by entering said security policy through a GUI at said client and server node.

Claim 22 (original) The method as recited in claim 19, wherein said policy database in said client and server node are configured by entering said security policy through a command line interface at said client and server node.

Claim 23 (original) The method as recited in claim 19, wherein said first ID is an ID of said particular member of said group name.

Claim 24 (currently amended) ~~The method as recited in claim 1 further comprising the step of:~~ A method for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name comprising the steps of:

configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name;

configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name;

establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy;

associating said tunnel with a group in said group database based on said member name such that only one copy of said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server node tunnels associated with said group; and

activating said tunnel, wherein activating tunnel comprises the steps of:

sending a security policy stored in a policy database of said client node by said client node to said server node;

sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security policy stored in said policy database of said client node;

sending a first nonce by said client node to said server node;

sending a second nonce by said server node to said client node;

sending a first ID by said client node to said server node; and

sending a second ID by said server node to said client node.

Claim 25 (original) A network system comprising:

a plurality of tunnels associated with a group name, wherein each of said plurality of tunnels associated with said group name comprises a plurality of nodes, wherein each of said plurality of nodes comprises a communication adapter to interconnect with said virtual private network, wherein one of said plurality of nodes is a server node, wherein one of said plurality of nodes is a client node, wherein said server node comprises:

a group database, wherein said group database comprises said group name and a list of members associated with said group name; and

a rules database, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name.

Claim 26 (original) The network system as recited in claim 25, wherein said server node further comprises:

a tunnel definition database, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name.

Claim 27 (original) The network system as recited in claim 26, wherein a particular tunnel of said plurality of tunnels associated with said group name is activated, wherein said particular tunnel is associated with a particular member of said group name.

Claim 28 (original) The network system as recited in claim 25, wherein said list of members associated with said group name comprise an ID type and an ID of each member associated with said group name.

Claim 29 (original) The network system as recited in claim 28, wherein said ID type is an Internet Key Exchange (IKE) defined ID type, wherein said list of members is a non-contiguous list of IKE defined ID types.

Claim 30 (original) The network system as recited in claim 28, wherein said ID is a login ID.

Claim 31 (original) The network system as recited in claim 28, wherein said ID is a specified name.

Claim 32 (original) The network system as recited in claim 26, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a GUI.

Claim 33 (original) The network system as recited in claim 26, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a command line interface.

Claim 34 (original) The network system as recited in claim 25, wherein said group database in said server node comprises said group name and an ID type of each member of said group name and an ID of each member of said group name.

Claim 35 (original) The network system as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a GUI.

Claim 36 (original) The network system as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a command line interface.

Claim 37 (original) The network system as recited in claim 34, wherein said group database in said server node is configured by a user entering said group name, said ID type of each member of said group name and said ID of each member of said group name through configuration files.

Claim 38 (original) The network system as recited in claim 25, wherein said rules database in said server node comprises said group name, a group name ID type and a security policy pointer.

Claim 39 (original) The network system as recited in claim 38, wherein said rules database is configured by a user entering said group name, said group name ID type and said security policy pointer through a GUI.

Claim 40 (original) The network system as recited in claim 39, wherein said rules database is configured by a user entering said group name, said group name ID type and said security policy pointer through a command line interface.

Claim 41 (currently amended) ~~The network system as recited in claim 27,~~ A network system comprising:

a plurality of tunnels associated with a group name, wherein each of said plurality of tunnels associated with said group name comprises a plurality of nodes, wherein each of said plurality of nodes comprises a communication adapter to interconnect with said virtual private network, wherein one of said plurality of nodes is a server node, wherein one of said plurality of nodes is a client node, wherein said server node comprises:

a group database, wherein said group database comprises said group name and a list of members associated with said group name; and

a rules database, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name;

wherein said server node further comprises:

a tunnel definition database, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name;

wherein a particular tunnel of said plurality of tunnels associated with said group name is activated, wherein said particular tunnel is associated with a particular member of said group name;

wherein activating said particular tunnel comprises the steps of:

sending a security policy stored in a policy database of said client node by said client node to said server node;

sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node;

sending a first nonce by said client node to said server node;

sending a second nonce by said server node to said client node;

sending a first ID by said client node to said server node; and

sending a second ID by said server node to said client node.

Claim 42 (original) The network system as recited in claim 41, wherein said first and second nonce are used to generate key material for said server and client node, respectively.

Claim 43 (original) The network system as recited in claim 41, wherein said policy database in said client and server node are configured by entering said security policy through a GUI at said client and server node.

Claim 44 (original) The network system as recited in claim 41, wherein said policy database in said client and server node are configured by entering said security policy through a command line interface at said client and server node.

Claim 45 (original) The network system as recited in claim 41, wherein said first ID is an ID of said particular member of said group name.

Claim 46 (currently amended) ~~The network system as recited in claim 27,~~ A network system comprising:

a plurality of tunnels associated with a group name, wherein each of said plurality of tunnels associated with said group name comprises a plurality of nodes, wherein each of said plurality of nodes comprises a communication adapter to interconnect with said virtual private network, wherein one of said plurality of nodes

is a server node, wherein one of said plurality of nodes is a client node, wherein said server node comprises:

a group database, wherein said group database comprises said group name and a list of members associated with said group name; and

a rules database, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name;

wherein said server node further comprises:

a tunnel definition database, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name;

wherein a particular tunnel of said plurality of tunnels associated with said group name is activated, wherein said particular tunnel is associated with a particular member of said group name;

wherein activating said particular tunnel comprises the steps of:

sending a security policy stored in a policy database of said client node by said client node to said server node;

sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security policy stored in said policy database of said client node;

sending a first nonce by said client node to said server node;

sending a second nonce by said server node to said client node;

sending a first ID by said client node to said server node; and

sending a second ID by said server node to said client node.

Claim 47 (previously presented) A computer program product having a computer readable medium having computer program logic recorded thereon for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name, comprising:

programming operable for configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name;

programming operable for configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name;

programming operable for establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy; and

programming operable for associating said tunnel with a group in said group database based on said member name such that only one copy of said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server node tunnels associated with said group.

Claim 48 (original) The computer program product as recited in claim 47 further comprises:

programming operable for configuring a tunnel definition database in said server node, wherein a remote ID in said tunnel definition is defined as said group name, wherein said server node has a single tunnel definition for each of the plurality of tunnels associated with said group name.

Claims 49-50 (canceled)

Claim 51 (original) The computer program product as recited in claim 47, wherein said list of members associated with said group name comprise an ID type and an ID of each member associated with said group name.

Claim 52 (original) The computer program product as recited in claim 51, wherein said ID type is an Internet Key Exchange (IKE) defined ID type, wherein said list of members is a non-contiguous list of IKE defined ID types.

Claim 53 (original) The computer program product as recited in claim 51, wherein said ID is a login ID.

Claim 54 (original) The computer program product as recited in claim 51, wherein said ID is a specified name.

Claim 55 (previously presented) The computer program product as recited in claim 48, wherein configuring said tunnel definition database in said server node comprises:

programming operable for establishing said server node and said client node as the two end points of said tunnel.

Claim 56 (original) The computer program product as recited in claim 55, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a GUI.

Claim 57 (original) The computer program product as recited in claim 55, wherein said tunnel definition database in said server node is configured by a user entering a local ID, a local ID type, said remote ID and a remote ID type through a command line interface.

Claim 58 (original) The computer program product as recited in claim 47, wherein said group database in said server node comprises said group name and an ID type of each member of said group name and an ID of each member of said group name.

Claim 59 (original) The computer program product as recited in claim 58, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a GUI.

Claim 60 (original) The computer program product as recited in claim 58, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through a command line interface.

Claim 61 (original) The computer program product as recited in claim 58, wherein configuring said group database in said server node is accomplished by entering said group name, said ID type of each member of said group name and said ID of each member of said group name through configuration files.

Claim 62 (original) The computer program product as recited in claim 47, wherein said rules database in said server node comprises said group name, a group name ID type and a security policy pointer.

Claim 63 (original) The computer program product as recited in claim 62, wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a GUI.

Claim 64 (original) The computer program product as recited in claim 62, wherein configuring said rules database in said server node is accomplished by entering said group name, said group name ID type and said security policy pointer through a command line interface.

Claim 65 (currently amended) ~~The computer program product as recited in claim 47 further comprising:~~ A computer program product having a computer readable medium having computer program logic recorded thereon for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name, comprising:

programming operable for configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name;

programming operable for configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name;

programming operable for establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy;

programming operable for associating said tunnel with a group in said group database based on said member name such that only one copy of said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server node tunnels associated with said group; and

programming operable for activating said tunnel, wherein said programming operable for activating said tunnel comprises:

programming operable for sending a security policy stored in a policy database of said client node by said client node to said server node;

programming operable for sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node matches said security policy stored in said policy database of said client node;

programming operable for sending a first nonce by said client node to said server node;

programming operable for sending a second nonce by said server node to said client node;

programming operable for sending a first ID by said client node to said server node; and

programming operable for sending a second ID by said server node to said client node.

Claim 66 (original) The computer program product as recited in claim 65, wherein said first and second nonce are used to generate key material for said server and client node, respectively.

Claim 67 (original) The computer program product as recited in claim 65, wherein said policy database in said client and server node are configured by entering said security policy through a GUI at said client and server node.

Claim 68 (original) The computer program product as recited in claim 65, wherein said policy database in said client and server node are configured by entering said security policy through a command line interface at said client and server node.

Claim 69 (original) The computer program product as recited in claim 65, wherein said first ID is an ID of said particular member of said group name.

Claim 70 (currently amended) ~~The computer program product as recited in claim 47 further comprising:~~ A computer program product having a computer readable medium having computer program logic recorded thereon for allowing a server node in a virtual private network to have a single tunnel definition and a single security policy for a plurality of tunnels associated with a group name, comprising:

programming operable for configuring a group database in said server node, wherein said group database in said server node comprises said group name and a list of members associated with said group name;

programming operable for configuring a rules database in said server node, wherein said rules database associates said group name with a particular security policy, wherein said server node has a single security policy for each of the plurality of tunnels associated with said group name;

programming operable for establishing a tunnel having a tunnel definition between a client node having a member name and said server node by negotiating a common security policy;

programming operable for associating said tunnel with a group in said group database based on said member name such that only one copy of said tunnel definition and associated security policy is maintained on said server node regardless of the number of client nodes to server node tunnels associated with said group; and

programming operable for activating said tunnel, wherein said programming operable for activating said tunnel comprises:

programming operable for sending a security policy stored in a policy database of said client node by said client node to said server node;

programming operable for sending a security policy stored in a policy database of said server node by said server node to said client node if said security policy stored in said policy database of said server node agrees on the same set of protection suites at any point in time with said security policy stored in said policy database of said client node;

programming operable for sending a first nonce by said client node to said server node;

programming operable for sending a second nonce by said server node to said client node;

programming operable for sending a first ID by said client node to said server node; and

programming operable for sending a second ID by said server node to said client node.